Notice of Allowability	Application No.	Applicant(s)	
	09/778,623	KO, CHEUK W.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *interview on 5/5/2005*.

2. ☒ The allowed claim(s) is/are *1,4-9,12-17,20-24 and 26-28*.

3. ☒ The drawings filed on *2/6/2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 5/5/2005
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

RD

DETAILED ACTION

Examiner's Amendment

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Kevin J. Zilka (Reg. No: 41,429) on 5/5/2005.

The application has been amended as follows:

3. Please replace claim 1 with the following:

A method for automatically generating a valid behavior specification for use in an intrusion detection system for a computer system, comprising:

receiving an exemplary set of system calls that includes positive examples of valid system calls, and possibly negative examples of invalid system calls; and

automatically constructing the valid behavior specification from the exemplary set of system calls by selecting a set of rules covering valid system calls;

wherein the set of rules covers all positive examples in the exemplary set of system calls without covering negative examples;

wherein selecting a rule for the valid behavior specification involves using an objective function that seeks to maximize the number of positive examples covered by the rule while seeking to minimize the number of possible system calls covered by the rule;

wherein the objective function additionally seeks to minimize the number of privileged system calls covered by the rule and minimize a length of the rule; and

wherein the objective function includes: $f_h = e_h - (g_h + p_h + c_h)$, where:

g_h = the generality of clause h;

p_h = the privilege of the clause h;

c_h = the length of clause h; and

e_h = the explanation power.

4. Please replace claim 9 with the following:

A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for automatically generating a valid behavior specification for use in an intrusion detection system for a computer system, the method comprising: receiving an exemplary set of system calls that includes positive examples of valid system calls, and possibly negative examples of invalid system calls; and automatically constructing the valid behavior specification from the exemplary set of system calls by selecting a set of rules covering valid system calls; wherein the set of rules covers all positive examples in the exemplary set of system calls without covering negative examples; wherein selecting a rule for the valid behavior

specification involves using an objective function that seeks to maximize the number of positive examples covered by the rule while seeking to minimize the number of possible system calls covered by the rule;

wherein the objective function additionally seeks to minimize the number of privileged system calls covered by the rule and minimize a length of the rule; and

wherein the objective function includes: $f_h = e_h - (g_h + p_h + c_h)$, where:

g_h = the generality of clause h;

p_h = the privilege of the clause h;

c_h = the length of clause h; and

e_h = the explanation power.

5. Please replace claim 17 with the following:

An apparatus that is configured to automatically generate a valid behavior specification for use in an intrusion detection system for a computer system, comprising: a receiving mechanism that is configured to receive an exemplary set of system calls that includes positive examples of valid system calls, and possibly negative examples of invalid system calls; and a specification construction mechanism that is configured to automatically construct the valid behavior specification from the exemplary set of system calls by selecting a set of rules covering valid system calls; wherein the set of rules covers all positive examples in the exemplary set of system calls without covering negative examples; wherein the specification construction mechanism is configured to select a rule for the valid behavior specification by using an objective function that seeks

to maximize the number of positive examples covered by the rule while seeking to minimize the number of possible system calls covered by the rule;

wherein the objective function additionally seeks to minimize the number of privileged system calls covered by the rule and minimize a length of the rule; and

wherein the objective function includes: $f_h = e_h - (g_h + p_h + c_h)$, where:

g_h = the generality of clause h;

p_h = the privilege of the clause h;

c_h = the length of clause h; and

e_h = the explanation power.

6. Please cancel claim 25.

7. Please replace claim 26 with the following:

The method of claim [[25]] 1, 9 and 17, wherein the values g_h and p_h are normalized to range from 1 to the total number of valid traces.

8. Please replace claim 28 with the following:

The method of claim [[25]] 1, 9 and 17, wherein the explanation power is a number of valid traces that can be at least partially explained by the clause *h*.

Allowable Subject Matter

9. Claims 1, 4 – 9, 12 – 17, 20 – 24 and 26 – 28 are allowed.

10. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claim 1 and subsequent dependent claims.

The CPA fails to teach or suggest a system for an apparatus that is configured to automatically generate a valid behavior specification for use in an intrusion detection system for a computer system, comprising: a receiving mechanism that is configured to receive an exemplary set of system calls that includes positive examples of valid system calls, and possibly negative examples of invalid system calls; and a specification construction mechanism that is configured to automatically construct the valid behavior specification from the exemplary set of system calls by selecting a set of rules covering valid system calls; wherein the set of rules covers all positive examples in the exemplary set of system calls without covering negative examples; wherein the specification construction mechanism is configured to select a rule for the valid behavior specification by using an objective function that seeks to maximize the number of positive examples covered by the rule while seeking to minimize the number of possible system calls covered by the rule; wherein the objective function additionally

seeks to minimize the number of privileged system calls covered by the rule and minimize a length of the rule; and wherein the objective function includes:

$f_h = e_h - (g_h + p_h + c_h)$, where:

g_h = the generality of clause h;

p_h = the privilege of the clause h;

c_h = the length of clause h; and

e_h = the explanation power.

Claims 9 and 17 and subsequent dependent claims would also be allowable for the reasons stated above

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100